МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №12 НА ТЕМУ:

Исследование стеганографического метода на основе преобразования наименее значащих битов

Выполнила студентка 3 курса 1 группы

Пригодич Вера Валерьевна

Минск 2023

Цель: изучение стеганографического метода встраивания\* /извлечения тайной информации с использованием электронного файлаконтейнера на основе преобразования наименее значащих битов (НЗБ), приобретение практических навыков программной реализации данного метода.

**Теоретические сведения**

Стеганографическая система (stegosystem, стегосистема или стеганосистема) – совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.

Основные компоненты стеганосистемы:

• контейнер С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение *М*; именно контейнер является упомянутым скрытым каналом;

• тайное сообщение *М*, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер; здесь речь может идти о невидимых цифровых водяных знаках (ЦВЗ));

• ключи, или ключевая информация, *K* системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом встраивания/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий – для предварительного (перед встраиванием) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;

• контейнер со встроенным сообщением, или стеганоконтейнер, *S*, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

• для полноты упомянем также субъектов системы: отправителя и получателя.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

• аудиостеганография;

• видеостеганография;

• графическая стеганография;

• текстовая стеганография;

• и др.

При построении стеганосистемы должны учитываться следующие основные положения:

• свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле; это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стеганосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего;

• противник (интруз) имеет полное представление о стеганографической системе и деталях ее реализации; единственной информацией, которая остается ему неизвестной, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

• если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения до тех пор, пока ключ хранится в тайне;

• потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука.

Рассмотрим это на примере 24-битного растрового RGB-изображения. Как известно, каждая точка кодируется тремя байтами. Каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цветов. Совокупность интенсивностей цвета в каждом из трех каналов определяет оттенок пикселя.

Младшие биты дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

**Практическое задание**

Разработать собственное приложение, в котором должен быть реализован метод НЗБ. При этом:

• выбор файла-контейнера – по согласованию с преподавателем;

В качестве типа файла-контейнера были выбраны изображения. Незаполненный контейнер имеет вид, показанный на рисунке 1.



Рисунок 1 – Вид «пустого» контейнера

• реализовать два варианта осаждаемого/извлекаемого сообщения:

− собственные фамилия, имя и отчество;

− текстовая часть отчета по одной из выполненных лабораторных работ;

Была использована текстовая часть отчета по лабораторной работе №2 на английском языке для удобства кодирования.

• реализовать два метода (на собственный выбор) размещения битового потока осаждаемого сообщения по содержимому контейнера;

Было реализовано осаждение по методу НЗБ с ключом и без.

Каждый восьмой бит пиксельного канала изображения заменяется на бит сообщения.

Для реализации НЗБ без ключа функция проходит через все пиксели изображения, изменяя значения компонент RGB каждого пикселя таким образом, чтобы в них были закодированы биты данных. Для каждого пикселя функция берет первые три компонента RGB и повторяет эту операцию три раза. Затем функция сравнивает каждый бит данных с младшим битом каждой компоненты пикселя и изменяет его, если необходимо.

Для получения сообщения из изображения программа проходит через пиксели и извлекает скрытые данные путем чтения младших битов компонент RGB каждого пикселя и преобразования их обратно в символы.

Реализация приведена в листинге 1.

def encode(message, img\_path, new\_img\_path):

    image = Image.open(img\_path, 'r')

    if (len(message) == 0):

        raise ValueError('Message is empty')

    newimg = image.copy()

    hide\_message(newimg, message)

    newimg.save(new\_img\_path, str(new\_img\_path.split(".")[1].upper()))

def decode(path):

    image = Image.open(path, 'r')

    data = ''

    imgdata = iter(image.getdata())

    while (True):

        pixels = [value for value in (

            imgdata.\_\_next\_\_()[:3] +

            imgdata.\_\_next\_\_()[:3] +

            imgdata.\_\_next\_\_()[:3]

        )]

        binstr = ''

        for i in pixels[:8]:

            if (i % 2 == 0):

                binstr += '0'

            else:

                binstr += '1'

        data += chr(int(binstr, 2))

        if (pixels[-1] % 2 != 0):

            return data

Листинг 1 – Реализация НЗБ без ключа

Результат осаждения ФИО представлен на рисунке 2.



Рисунок 2 – Контейнер с ФИО

Результат осаждения отчета представлен на рисунке 3.



Рисунок 3 – Контейнер с отчетом

Для реализации НЗБ с ключом используется генерация случайного ключа в пределах ширины и высоты изображения, и значение RGB пикселя по этому ключу изменяется, чтобы закодировать символ. Ключи записываются в текстовый файл, и новое изображение сохраняется.

Для получения сообщения из изображения изображение открывается и загружаются пиксели. Затем считываются ключи из файла и восстанавливаются закодированные значения символов из пикселей, используя ключи. Возвращается декодированное сообщение в виде строки символов.

Реализация приведена в листинге 2.

def encode(message, img\_path, new\_img\_path, key\_path):

    keys = []                   #сюда будут помещены ключи

    img = Image.open(img\_path)  #создаём объект изображения

    draw = ImageDraw.Draw(img)          #объект рисования

    width = img.size[0]                 #ширина

    height = img.size[1]                #высота

    pix = img.load()                #все пиксели тут

    f = open(key\_path,'w')          #текстовый файл для ключей

    for elem in ([ord(elem) for elem in message]):

        key = (randint(1,width-10),randint(1,height-10))

        g, b = pix[key][1:3]

        draw.point(key, (elem,g , b))

        f.write(str(key)+'\n')

    print(f'keys were written to the  {key\_path} file')

    img.save(new\_img\_path, "PNG")

    f.close()

def decode(img\_path, key\_path):

    a = []

    keys = []

    img = Image.open(img\_path)

    pix = img.load()

    f = open(key\_path,'r')

    y = str([line.strip() for line in f])

    for i in range(len(findall(r'\((\d+)\,',y))):

        keys.append((int(findall(r'\((\d+)\,',y)[i]),int(findall(r'\,\s(\d+)\)',y)[i])))

    for key in keys:

        a.append(pix[tuple(key)][0])

    return ''.join([chr(elem) for elem in a])

Листинг 2 – Реализация НЗБ с ключом

Результат осаждения ФИО представлен на рисунке 4.



Рисунок 4 – Контейнер с ФИО

Результат осаждения отчета представлен на рисунке 5.



Рисунок 5 – Контейнер с отчетом

• выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе выполненного анализа.

Визуальный анализ показал, что человеческий глаз не может определить различия между пустым контейнером и контейнером с сообщением.

Вывод: В ходе лабораторной работы было разработано приложение, позволяющее скрывать сообщения с помощью метода преобразования наименее значащих битов в изображениях.

**Контрольные вопросы**

1. Охарактеризовать цели, задачи и области применения стеганографии.

Цель – скрыть факт передачи сообщения.

Задачи – разработка методов, позволяющих выполнить цель.

Область применения – информационная безопасность и криптография, когда скрытая информация может быть использована для хранения секретных данных, обеспечения безопасности сети или транспортировки сообщений в условиях, когда прямая передача информации затруднена или нежелательна.

1. В чем состоят сходства и различия между стеганографией и криптографией?

Целью криптографии является преобразование информации в такой вид, при котором её сложно прочитать, не имея ключевой информации и понимания работы криптографического алгоритма. Целью же стеганографии является сокрытие факта передачи информации.

1. Дать определение стеганографической системы. Охарактеризовать составные части стеганосистемы и их взаимосвязь.

Стеганографическая система (stegosystem, стегосистема или стеганосистема)– совокупность средств и методов, которые используются для формирования скрытого канала передачи (или хранения) информации.

Основные компоненты стеганосистемы:

• контейнер С (файл-контейнер или электронный документ произвольного формата), в котором размещается (осаждается, скрывается) тайное сообщение *М*; именно контейнер является упомянутым скрытым каналом;

• тайное сообщение *М*, осаждаемое в контейнер для передачи или хранения (например, с целью доказательства или защиты авторских прав на документ-контейнер; здесь речь может идти о невидимых цифровых водяных знаках (ЦВЗ));

• ключи, или ключевая информация, *K* системы, выполняющие ту же функцию, что и криптографические ключи; ключей может быть несколько, в соответствии с этим современные стеганосистемы характеризуют как многоключевые: один ключ отождествляется с методом встраивания/извлечения тайной информации, другой – с выбором элементов (например, битов) контейнера для его модификации при осаждении тайной информации, третий – для предварительного (перед встраиванием) преобразования тайной информации (например, на основе помехоустойчивого кодирования, сжатия или зашифрования) и т. д.;

• контейнер со встроенным сообщением, или стеганоконтейнер, *S*, который передается по открытому каналу, также являющемуся важным компонентом анализируемой системы; стеганоконтейнер будем именовать также стеганосообщением;

• для полноты упомянем также субъектов системы: отправителя и получателя.

1. Основные классификационные критерии методов стеганографии.

В зависимости от формата документа-контейнера цифровую (или компьютерную) стеганографию подразделяют на классы:

• аудиостеганография;

• видеостеганография;

• графическая стеганография;

• текстовая стеганография;

• и др.

1. Пояснить сущность основных атак на стеганосистемы.

* по известному заполненному контейнеру;
* по известному встроенному сообщению;
* на основе выбранного скрытого сообщения;
* на основе выбранного заполненного контейнера;
* на основе известного пустого контейнера;
* на основе выбранного пустого контейнера;
* по известной математической модели контейнера.

1. Изобразить структурную схему стеганографической системы.

Структурная схема стеганографической системы имеет следующий вид:

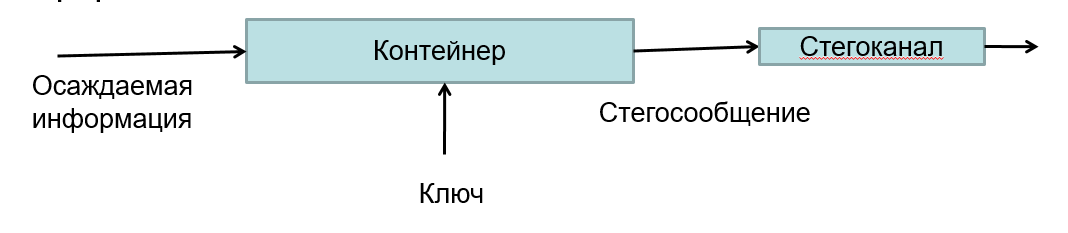


Рисунок ­- Структурная схема стеганографической системы

1. Сущность метода НЗБ. Области его применении.

Метод НЗБ основывается на ограниченных способностях зрения или слуха человека, вследствие чего людям тяжело различать незначительные вариации цвета или звука. Младшие биты (выделены бледным, справа) дают незначительный «вклад» в изображение по сравнению со старшими. Замена одного или даже нескольких младших битов для человеческого глаза будет почти незаметна, поскольку реально человек может различать около полторы сотни цветовых оттенков.

Области применения метода LSB в стеганографии включают:

1. Защита авторских прав - в стеганографическом изображении можно скрыть информацию о правообладателе, дате создания, лицензии и т.д. Это позволяет защитить авторские права на изображение и легализовать его использование.
2. Безопасность данных - метод LSB может использоваться для скрытия конфиденциальной информации в видео- или аудиофайлах, что позволяет обмениваться информацией без вызова подозрений у третьих лиц.
3. Маркирование изображений - метод LSB может использоваться для маркирования изображений, чтобы облегчить их последующее распознавание и идентификацию.
4. Контроль и наблюдение - метод LSB может использоваться для контроля и наблюдения за сотрудниками, например, для отслеживания активности в интернете и нежелательного использования корпоративных ресурсов.
5. Скрытый обмен сообщениями - метод LSB может использоваться для скрытого обмена сообщениями в условиях, когда прямая передача информации затруднена или нежелательна.
6. Восстановление поврежденных данных - метод LSB может использоваться для восстановления поврежденных данных, если в них была скрыта дополнительная информация.
7. Контроль целостности данных - метод LSB может использоваться для контроля целостности данных, т.е. проверки, не были ли изменены данные в процессе передачи или хранения.
8. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при передаче этих сообщений.

Алгоритм встраивания:

1. Перевести сообщение в бинарный вид;

2. Перевести контейнер в бинарный вид и разбить его на сегменты по n бит;

3. Заменять младшие биты каждого сегмента битами сообщения, пока сообщение не закончится. Заменять можно от 1 до n-1 младших бит сегмента;

4. Перевести бинарный вид контейнера к изначальному формату.

Алгоритм извлечения:

1. Перевести контейнер в бинарный вид и разбить его на сегменты по n бит;

2. Извлечь из каждого сегмента от 1 до n-1 младших бит (число извлекаемых является заранее известным);

3. Сконкатенировать извлечённые биты;

4. Привести полученную бинарную последовательность к изначальному формату сообщения.

1. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при решении задачи защиты прав интеллектуальной собственности на электронный контент.

Алгоритм встраивания сообщений на основе метода НЗБ:

1. Прочитать оригинальный электронный контент (например, изображение) и сообщение, которое нужно встроить.
2. Преобразовать сообщение в последовательность битов.
3. Пройтись по каждому пикселю (или блоку пикселей) в оригинальном контенте.
4. Для каждого пикселя, взять его значения цветовых компонент (например, красной, зеленой и синей) и изменить младший бит каждой компоненты на соответствующий бит из сообщения.
5. Повторить шаги 3-4 для всех пикселей или блоков пикселей, встраивая сообщение постепенно.
6. Сохранить измененный электронный контент с встроенным сообщением.

Алгоритм извлечения сообщений на основе метода НЗБ:

1. Прочитать электронный контент с встроенным сообщением.
2. Пройтись по каждому пикселю (или блоку пикселей) в измененном контенте.
3. Для каждого пикселя, взять младший бит каждой цветовой компоненты и сохранить его.
4. Собрать все сохраненные биты в последовательность.
5. Преобразовать последовательность битов в сообщение.
6. Извлеченное сообщение теперь доступно для дальнейшего использования или анализа.